Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fred Horvat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe, log on to our website at: www.atarinews.org and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to subscribe from.

To download A-ONE, set your browser bookmarks to one of the following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

A-ONE #1748 12/25/15

~ Oracle Gets Java Order! ~ People Are Talking! ~ Apple Blasts UK Bill
~ French Sue Over Steam! ~ Facebook India Trouble ~ Error Code 451!
~ 1st Web Site 25 Yrs Ago ~ Secret Code in Juniper ~ Firebee News Update!

~ Google vs. Passwords! ~ No More Non-touch PCs? ~ Zero Three Zero!

-* Gamers: 50% Play, 10% Identify* -
-* Downloads: A Gaming Turning Point! *-
-* Millions To Lose Secure Internet Access! *-

=~=~=~=

->From the Editor’s Keyboard "Saying it like it is!"
""""""""""""""""""""""""""""

Happy Holidays everyone!! I hope that everybody had a great Hanukkah or Christmas! I enjoyed both! And, there was none of that cold, wet, white stuff on the ground this year! In fact, we were in the 60’s in my neck of the woods. Personally, I have no problem celebrating a brown holiday!

This is the last issue for the year, so I’ll wish everyone a Happy New Year now. Stay safe,and celebrate the holidays with a good degree of responsibility!

Until next year...

=~=~=~=

FireBee News Update

By Fred Horvat

Last submission I posted my DIP Switch settings to http://www.atari-forum.com/viewtopic.php?f=92&t=28704&start=25 . It was suggested that I put Switch #5 to the Off (down) setting while #6 was still On (up). That would give me : -) Run EmuTOS in fully ColdFire native mode (DIP switch No. 5 down, No. 6 up) as stated from the FireBee Page http://firebee.org/fb-bin/page?label=fb_pinout&lng=en .

I did this and the FireBee chirps nonstop like a stuck key on the keyboard and goes straight to the ColdBoot menu and locks up. I set the settings back to what they were prior with both 5 and 6 UP and the system will not boot now to the CF. It starts booting and when it starts reading from the AUTO Folder the system does a reboot.

I tried my spare CF with a fresh install of MiNT that I have and it did the same thing so it appears that the CF card is not

corrupt.

Looks like I will have to reflash the FireBee again and hopefully
that will straighten things out.

And that s where I left it for now. With the holidays I didn t
get a whole lot of time to put towards the FireBee. I want to get
it back to where it was before in running FreeMiNT 1.18 that came
on the FireBee. Eventually I d like to run EasyMiNT with the
newer FreeMiNT 1.19 and SpareMiNT to give me more Unix capability
but first thing first.

Zero Three Zero

Francois Le Coat

Hi,

Merry Christmas...

Zero Three Zero - Atari Falcon030 demo by The Pixel Twins
and Excellence in Art

        <http://www.youtube.com/watch?v=K9vUfsZ3eiY>

Presented at ST News International Christmas Coding Convention
2015.
Capture from emulator at 50fps. Enjoy!

ATARIstically yours =)

--
François Le Coat
Author of Eureka 2.12 (2D Graph Describer, 3D Modeller)
http://eureka.atari.org/

=~=~=~=

->In This Week’s Gaming Section - Downloads: Turning Point for Game Industry!
  """""""""""""""""""""""""""""""   French Sue To Re-sell Steam Games!
                                    50% Play, 10% Identify As Gamers!

=~=~=~=

->A-ONE’s Game Console Industry News   - The Latest Gaming News!
  """""""""""""""""""""""""""""""""""

As Downloads Take Over, A Turning Point for the Video Game Industry

This holiday season could be remembered as a digital watershed for the games business, the moment when the old way of selling video games on discs in boxes finally gave way to downloads.

The industry has been pointed in this direction for years. But the signs of a sharp turning point have piled up in the last month, as new data points have painted conflicting pictures of the game industry.

On one hand, recent market research shows that physical game sales declined in November, and GameStop, a leading retailer, reported disappointing earnings that made its stock tumble.

On the other, game companies swear that things are going great. Big titles are setting sales records, and Sony, the leading maker of game consoles, says the latest PlayStation has been selling at a faster clip than any previous generation of the hardware.

Why the disparity?

A number of factors are at play, but none as significant as the industry s march toward a future of games downloaded over the Internet rather than bought in stores, analysts said. All mobile games are delivered over the Internet, as are nearly all PC games. But the transition for console games the biggest segment of the business has been far slower. Large game files could take hours to download and quickly fill a console s hard drive.

Now, faster broadband speeds and the bigger hard drives in the latest generation of consoles are reducing those obstructions.

It finally feels like the inevitable is becoming the inevitable, said Evan Wilson, an analyst who follows the game industry for Pacific Crest Securities. It feels like this is the holiday season where it s finally having a big impact.

Electronic Arts, the big games publisher behind Madden and Need for Speed, says about 20 percent of its new console games are now downloaded, compared with around 10 to 15 percent last year. For other publishers, the number may be 25 percent or more.

As a result, it is becoming harder to judge the health of the industry based on sales of physical game discs. NPD Group, a research firm that tracks retail sales in the United States, showed a 7 percent decline in November game sales from the same month a year ago.

Mr. Wilson of Pacific Crest characterized the figures in the title of a research report: Shockingly Bad NPD Data Shows Big Physical Challenges.

A couple of weeks earlier, there was similarly grim news from GameStop, the big specialty retailer, which blamed a disappointing earnings report for the period ending Oct. 31 on

weak new game software and hardware sales.

Executives at GameStop caused a further stir when they said one of the most anticipated games of the season, Star Wars: Battlefront, had missed their internal sales forecasts during the quarter. The stock of Electronic Arts, the game s publisher, fell 5 percent the day of the remarks.

The numbers were particularly striking because if game sales are ever going to grow, the time is now. The biggest games of the year have just landed on store shelves including Fallout 4, Call of Duty: Black Ops 3, and Star Wars: Battlefront and demand for them is running high among holiday gift buyers.

What is more, the industry is in the sweet spot of the hardware cycle, when the latest consoles from Sony and Microsoft are in plentiful supply and their prices have come down, and game publishers are cranking out titles that better exploit their capabilities.

Sony, for one, says its console sales have never been better. The company reported that it sold 30.2 million PlayStation 4s worldwide as of late November, just days after the second anniversary of the product. By comparison, it took around two years and two months for Sony to ship about 30 million PlayStation 2s the previous high-water mark for Sony in the game business.

One factor in NPD s declining game sales is that the research firm does not include games that are bundled with consoles an increasingly popular option for buying the machines in its software sales data. But a much bigger reason is that it does not include digital downloads of games in its monthly tallies of the industry.

Liam Callahan, an analyst at NPD, said the firm includes digital sales in a game report that comes out every quarter. For the first nine months of the year, game spending on physical formats was flat compared with the same period in 2014. When digital sales were included, there was an 8 percent increase, he said.

 It s clear digital downloading is becoming a bigger deal, said Michael Pachter, an analyst at Wedbush Securities.

After GameStop s comments about Star Wars: Battlefront rattled investors, a senior executive at Electronic Arts, Peter Moore, said at a conference that there was no weakness that is perceptible yet in the title. He reiterated the company s previous projection that it would sell 13 million copies of the game during its fiscal year.

The bigger threat appears to be for retailers that fail to adjust to the changing market. The list of retailers that have been vaporized by the Internet is long, including Blockbuster in movies, Tower Records in music and Virgin Megastores in both.

GameStop has increased its own presence in Internet-delivered games, but those changes have not moved the needle much. The company s digital revenue in its last quarter amounted to less than 2 percent of its total revenue. There are limits to how much

the company can sell digitally, though, since Microsoft, Sony and Nintendo operate the online portals from which the games are downloaded.

GameStop has tried to diversify beyond video games by acquiring one retail chain that offers wireless products and another that sells and repairs Apple devices. Joey Mooring, a spokesman for GameStop, said the company s in-store staff members provide guidance for customers. And through its trade-in program for used games, customers can get credits toward the purchase of new games.

Customers cannot access that expertise downloading a game, nor can they trade in a digital game for currency that can be applied to the purchase of their next game, Mr. Mooring said in an email.

Eric Lempel, senior vice president for marketing at Sony s American games division, agreed with the idea that many gamers want to talk to store staff members before making a purchase. The convenience of downloading a game directly to a console is appealing too, though.

A lot of people are finding it easier to buy online, Mr. Lempel said. It s open 24 hours a day.

French Consumer Group Sues for Right To Resell Steam Games

A French consumer group has brought a lawsuit against Valve, saying that Steam and its required terms of service infringe on a number of European legal rights, including the right to legally resell purchased software.

The 64-year-old UFC-Que Choisir (the "federal union of consumers") argues that Valve must provide the capability for Steam users to resell their legally purchased digital games whenever they want. While noting that many online stores have similar resale restrictions, the group argues that the difference between being able to resell a physical game disc and not being able to resell a digitally purchased game is "incomprehensible... No court decision prohibits the resale on the second-hand market games bought online, and the European Court has even explicitly stated that it s possible to resell software which, let s remember, is an integral part of a video game."

First-sale rights stronger in the EU than in the US.

The group is referring to a 2012 decision from the European Court of Justice that focused on the resale of downloadable enterprise software licensed from Oracle. "It makes no difference whether the copy of the computer program was made available by means of a download from the rightholder s website or by means of a material medium such as a CD-ROM or DVD," the court ruled.

"From an economic point of view, the sale of a computer program on CD-ROM or DVD and the sale of a program by downloading from the Internet are similar," the court ruled. "The on-line transmission

method is the functional equivalent of the supply of a material medium." But in 2014, the Regional Court of Berlin ruled in favor of Valve in a case brought by a German group arguing for the same resale rights.

The state of the law is quite different in the US, where courts have decided on multiple occasions that companies had broad rights to limit resale of digital software through the use of end-used license agreements, even for physical copies of software. That decision is in some conflict with the "first sale doctrine" that gives an initial purchaser wide-ranging rights regarding the use of a purchased product. Software publishers have argued successfully, in Vernor vs. Autodesk that software is licensed, not purchased, and therefore the doctrine of first sale does not apply.

Traded items will be "held" for days unless you have two-factor security.
In addition to the resale complaint, UFC-Que Choisir takes Valve to task for claiming the right to reuse any user-created content on Steam "at will." This clause "denies... respect for the users'/creators' rights of intellectual property," the group says. The group also wants Valve to accept some liability if and when users' personal data is hacked or breached from Valve's servers, specifically citing the 77,000 Steam accounts that Valve says are compromised every month.

UFC-Que Choisir also wants Valve to allow Steam users to refund remaining money out of their Steam Wallets when they close their accounts. Finally, the group disputes the use of Luxembourg law for any European complaints against the company. "We have the same currency but not the same rights!" the French group says.

UFC-Que Choisir says it had previously provided Valve with formal notice of its complaint and has brought the case to the High Court of Paris "in the face of resistance from Valve." Valve has yet to respond to a request for comment from Ars on the complaint.

50% of Americans Play Games But Only 10% Identify as Gamers

The good news in a survey conducted by Pew Research is that more people than ever are gaming; the bad news is only a fraction of them are willing to admit it.

According to the survey entitled Gaming and Gamers, 50% of American men and 48% of women play games, but only 10% self-identify as "gamers."

While the report doesn't directly theorize why such a small portion are willing to consider themselves gamers, it does note that "among the general public, attitudes towards games are complex and often uncertain." The survey shows equal percentages of respondents being diametrically opposed on questions like "are videogames a waste of time?" with 26% saying "true for most games," while 24% say "untrue for most games" and whether people who play violent video games are more likely to be violent themselves, with 40% of all adults agreeing with that statement and 53% disagreeing.

The survey also delves into representation with questions about whether most games portray women and minorities poorly. While 14% agreed that most videogames portrayed women poorly versus 18% that said most games do not, the majority at 40% stated they were unsure. While only 9% said they thought most games portrayed minorities poorly versus 23% who said most games do not, 47% were unsure.

Pew also found that despite 48% of women admitting to playing games, 60% of all respondents thought that the majority of people who play games are men. In a bit of unsurprising news, the survey said "fully 77% of men ages 18 to 29 play video games (more than any other demographic group)." While 57% of women in the same demo bracket also play games, only 9% of them identified as gamers.

Pew conducted the survey by phone over the summer with 2,001 people responding.

=~=~=~=

A-ONE's Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

Millions To Lose Secure Internet Access on January 1

Internet surfers may take that little green or gold lock in the corner of their Web browser for granted. But starting Jan. 1, it might go away for a small percentage of people across the globe, and millions of users could lose access to websites because of it.

It's all to do with the "SHA-1 Sunset," a phrase used by technology insiders to describe the expiration of support for a certain level of encryption. Over the next year, the algorithms older than SHA-1 level of encryption will no longer meet the trusted level of security for many websites, leaving as many as 37 million people unable to access them, according to research from Internet performance and security company CloudFlare.

It's a routine update to a Web feature called the certificate signature hashing algorithm. But the change, decided by a consortium of vendors of Internet browser software, could disproportionately affect mobile devices in the developing world.

As a result, some of the world's most vulnerable population will be left with only the selection of websites they can view without the needed safety protocols.

Here's how it works, according Tim Erlin, director of IT security and risk strategy at Tripwire.

When your website connects to a browser, each sends and receives

data. During the encryption process, the website and browser enter into a "conversation," to use a metaphor. When they do so, they negotiate a secret, secure code to "speak" in, that’s different for every conversation.

Part of the negotiation between the browser and website is to agree to use the most complex language that both parties can understand, Erlin said.

"Hackers break that algorithm," Erlin said. "Once its broken, it becomes much easier for a criminal to overhear your conversations. There should always be a plan to upgrade the algorithm because people are always looking to break it."

Luckily, most people are protected from these types of hackers without any action on their part, since many websites and browsers default to encrypted versions, signified by the "s" in "https://." Indeed, if you’re using an up-to-date browser, you probably were automatically upgraded to at least SHA-2 level algorithms, Erlin said.

But older operating systems and browsers, such as Windows XP, may no longer support updates to newer encryption levels, said Erlin. And more encryption requires more processing power, leaving older mobile devices, mostly used in developing countries, too jammed up to handle secure browsing.

That may leave users with phones older than five years with an error message when they try to access sites that don’t offer un-encrypted versions a decision that varies for each individual site, Erlin said.

SHA-2 support in Western Europe and North America is universally more than 99 percent, according to new CloudFlare research. But closer to 5 percent of Internet users in countries like China, Cameroon, Yemen, Sudan, Egypt and Libya user browsers without SHA-2 support.

"When you trade in your cellphone in a country like United States, those cellphones make their way to the developing world," Matthew Prince, co-founder of CloudFlare, told CNBC’s on Monday. "And those phones are ending up in the hands of people who now won’t be able to access parts of the encrypted Internet."

Worldwide, a population roughly the size of California doesn’t have the needed support, CloudFlare estimates.

"Unfortunately, this list largely overlaps with lists of the poorest, most repressive, and most war-torn countries in the world," CloudFlare wrote. "In other words, after Dec. 31, most of the encrypted Web will be cut off from the most vulnerable populations of Internet users who need encryption the most. And, unfortunately, if we’re going to bring the next 2 billion Internet users online, a lot of them are going to be doing so on secondhand Android phones, so this problem isn’t going away anytime soon."

Because SHA-2 support is more limited than during previous certificate signature hashing algorithm upgrades, technology companies have been forced to debate an "appropriate balance between two desirable goals ... making systems secure against new

attacks and providing security to the broadest population," wrote Facebook’s chief security officer, Alex Stamos, .

Google has been the most aggressive at turning off the old encryption support. Alibaba, on the other hand, has made sure its sites fall back to support the older versions of encryption technology, Prince said.

"We will continue to have to deprecate older standards, and move to new standards as computers get faster over the next few years," Prince said. "You’ll see some of these users with the older phones having a new incentive to go and upgrade. But obviously, in places like Syria, where over 4 percent of users will suddenly lose access to encryption, they’re not going to be running down to their AT&T store to get new phones."

While Facebook sees the need for the upgrade, Stamos expressed doubts for the way the changeover is being carried out. But he acknowledged many well-meaning people disagree with Facebook’s proposed workaround: a new type of legacy certificate.

"We don’t think it’s right to cut tens of millions of people off from the benefits of the encrypted Internet, particularly because of the continued usage of devices that are known to be incompatible with SHA-256," Stamos wrote. "Many of these older devices are being used in developing countries by people who are new to the Internet. ... We should be investing in privacy and security solutions for these people, not making it harder for them to use the Internet safely."

How Websites Will Signal When They’re Censored

A new error code, known as 451, could signal that the Web page you re after has been censored.

Governments will not always be able to disguise which content they restrict across the Web thanks to a new error code that will warn you of censorship.

The Internet serves up a range of status codes, numbered from the 100s to the 500s, to let you know when something goes wrong, such as server downtime, to keep you from getting to a given Web page. You re likely familiar with the common 404 error message that tells you a page cannot be found.

It isn t always easy, however, to work out whether a Web page is down because of technical hiccups or governmental meddling. That s where the new 451 code comes in.

On Friday, the group responsible for Internet standards, the Internet Engineering Steering Group, approved a new HTTP code to differentiate between Web pages that cannot be shown for technical reasons and others that are unavailable for non-technical reasons, such as censorship.

The Internet has long been a target of censors. Governments in the European bloc force Internet service providers to restrict access

to websites linking to pirated content, China has a Great Firewall that heavily restricts the Web, and countries including Russia and South Korea are known for cracking down on access.

Mark Nottingham, chair of the group of developers who oversee the Web s core protocol known as HTTP, explained in a blog post while the existing 403 error status code says Forbidden, it does not specify whether there are legal reasons for restricting content.

However, status code 451   a hat tip to Fahrenheit 451, the classic Ray Bradbury tale about a futuristic society fixated on book-burning   can now be used to distinguish pages unavailable due to censorship.

 As censorship became more visible and prevalent on the Web, we started to hear from sites that they d like to be able to make this distinction, Nottingham said.

In addition, some organizations said they would like to be able to search the Web for pages containing a censorship-based error code in order to catalog examples of censorship.

Nottingham predicts that the 451 code will likely be used more on Web servers than by network-based intermediaries, as websites including Twitter, Facebook, Google and Github are forced to censor content in certain countries and jurisdictions.

There are also discussions under way concerning how 451 could be used to prompt users to access restricted content in other ways.

 In some jurisdictions, Nottingham wrote, I suspect that censorious governments will disallow the use of 451, to hide what they re doing. We can t stop that (of course), but if your government does that, it sends a strong message to you as a citizen about what their intent is. That s worth knowing about, I think.

Secret Code Found in Juniper s Firewalls Shows Risk of Government Backdoors

Encryption backdoors have been a hot topic in the last few years and the controversial issue got even hotter after the terrorist attacks in Paris and San Bernardino, when it dominated media headlines. It even came up during this week s Republican presidential candidate debate. But despite all the attention focused on backdoors lately, no one noticed that someone had quietly installed backdoors three years ago in a core piece of networking equipment used to protect corporate and government systems around the world.

On Thursday, tech giant Juniper Networks revealed in a startling announcement that it had found unauthorized code embedded in an operating system running on some of its firewalls.

The code, which appears to have been in multiple versions of the company s ScreenOS software going back to at least August 2012, would have allowed attackers to take complete control of Juniper

NetScreen firewalls running the affected software. It also would allow attackers, if they had ample resources and skills, to separately decrypt encrypted traffic running through the Virtual Private Network, or VPN, on the firewalls.

During a recent internal code review, Juniper discovered unauthorized code in ScreenOS that could allow a knowledgeable attacker to gain administrative access to NetScreen devices and to decrypt VPN connections, Bob Worrall, the companies CIO wrote in a post. Once we identified these vulnerabilities, we launched an investigation into the matter, and worked to develop and issue patched releases for the latest versions of ScreenOS.

'This is a very good showcase for why backdoors are really something governments should not have in these types of devices because at some point it will backfire.'

Juniper released patches for the software yesterday and advised customers to install them immediately, noting that firewalls using ScreenOS 6.2.0r15 through 6.2.0r18 and 6.3.0r12 through 6.3.0r20 are vulnerable. Release notes for 6.2.0r15 show that version being released in September 2012, while release notes for 6.3.0r12 show that the latter version was issued in August 2012.

The security community is particularly alarmed because at least one of the backdoors appears to be the work of a sophisticated nation-state attacker.

The weakness in the VPN itself that enables passive decryption is only of benefit to a national surveillance agency like the British, the US, the Chinese, or the Israelis, says Nicholas Weaver, a researcher at the International Computer Science Institute and UC Berkeley. You need to have wiretaps on the internet for that to be a valuable change to make [in the software].

But the backdoors are also a concern because one of them a hardcoded master password left behind in Juniper s software by the attackers will now allow anyone else to take command of Juniper firewalls that administrators have not yet patched, once the attackers have figured out the password by examining Juniper s code.

Ronald Prins, founder and CTO of Fox-IT, a Dutch security firm, said the patch released by Juniper provides hints about where the master password backdoor is located in the software. By reverse-engineering the firmware on a Juniper firewall, analysts at his company found the password in just six hours.

Once you know there is a backdoor there, the patch [Juniper released] gives away where to look for [the backdoor] which you can use to log into every [Juniper] device using the Screen OS software, he told WIRED. We are now capable of logging into all vulnerable firewalls in the same way as the actors [who installed the backdoor].

But there is another concern raised by Juniper s announcement and patches any other nation-state attackers, in addition to the culprits who installed the backdoors, who have intercepted and stored encrypted VPN traffic running through Juniper s firewalls

in the past, may now be able to decrypt it, Prins says, by analyzing Juniper s patches and figuring out how the initial attackers were using the backdoor to decrypt it.

If other state actors are intercepting VPN traffic from those VPN devices, they will be able to go back in history and be able to decrypt this kind of traffic, he says.

Weaver says this depends on the exact nature of the VPN backdoor. If it was something like the Dual EC, the backdoor doesn t actually get you in, you also need to know the secret. But if it s something like creating a weak key, then anybody who has captured all traffic can decrypt. Dual EC is a reference to an encryption algorithm that the NSA is believed to have backdoored in the past to make it weaker. This factor, along with knowledge of a secret key, would allow the agency to undermine the algorithm.

Matt Blaze, a cryptographic researcher and professor at the University of Pennsylvania, agrees that the ability to decrypt already-collected Juniper VPN traffic depends on certain factors, but cites a different reason.

If the VPN backdoor doesn t require you to use the other remote-access [password] backdoor first, then it would be possible to decrypt historical traffic that had been captured, he says. But I can imagine designing a backdoor in which I have to log into the box using the remote-access backdoor in order to enable the backdoor that lets me decrypt intercepted traffic.

A page on Juniper s web site does appear to show that it s using the weak Dual EC algorithm in some products, though Matthew Green, a cryptography professor at Johns Hopkins University, says it s still unclear if this is the source of the VPN issue in Juniper s firewalls.

Juniper released two announcements about the problem on Thursday. In a second more technical advisory, the company described two sets of unauthorized code in the software, which created two backdoors that worked independently of one another, suggesting the password backdoor and the VPN backdoor aren t connected. A Juniper spokeswoman refused to answer questions beyond what was already said in the released statements.

Regardless of the precise nature of the VPN backdoor, the issues raised by this latest incident highlight precisely why security experts and companies like Apple and Google have been arguing against installing encryption backdoors in devices and software to give the US government access to protected communication.

This is a very good showcase for why backdoors are really something governments should not have in these types of devices because at some point it will backfire, Prins says.

Green says the hypothetical threat around NSA backdoors has always been: What if someone repurposed them against us? If Juniper did use Dual EC, an algorithm long-known to be vulnerable, and this is part of the backdoor in question, it underscores that threat of repurposing by other actors even more.

The use of Dual EC in ScreenOS should make us at least consider the possibility that this may have happened, he told WIRED.

The first backdoor Juniper found would give an attacker administrative-level or root privileges over the firewalls essentially the highest-level of access on a system when accessing the firewalls remotely via SSH or telnet channels. Exploitation of this vulnerability can lead to complete compromise of the affected system, Juniper noted.

Although the firewall s log files would show a suspicious entry for someone gaining access over SSH or Telnet, the log would only provide a cryptic message that it was the system that had logged on successfully with a password. And Juniper noted that a skilled attacker would likely remove even this cryptic entry from log files to further eliminate any indication that the device had been compromised.

The second backdoor would effectively allow an attacker who has already intercepted VPN traffic passing through the Juniper firewalls to decrypt the traffic without knowing the decryption keys. Juniper said that it had no evidence that this vulnerability had been exploited, but also noted that, There is no way to detect that this vulnerability was exploited.

Juniper is the second largest maker of networking equipment after Cisco. The Juniper firewalls in question have two functions. The first is to ensure that the right connections have access to a company or government agency s network; the other is to provide secured VPN access to remote workers or others with authorized access to the network. The ScreenOS software running on Juniper firewalls was initially designed by NetScreen, a company that Juniper acquired in 2004. But the versions affected by the backdoors were released under Juniper s watch, eight years after that acquisition.

The company said it discovered the backdoors during an internal code review, but it didn t say if this was a routine review or if it had examined the code specifically after receiving a tip that something suspicious was in it.

Speculation in the security community about who might have installed the unauthorized code centers on the NSA, though it could have been another nation-state actor with similar capabilities, such as the UK, China, Russia, or even Israel.

Prins thinks both backdoors were installed by the same actor, but also notes that the hardcoded master password giving the attackers remote access to the firewalls was too easy to find once they knew it was there. He expects the NSA would not have been so sloppy.

Weaver says it s possible there were two culprits. It could very well be that the crypto backdoor was [done by] the NSA but the remote-access backdoor was the Chinese or the French or the Israelis or anybody, he told WIRED.

NSA documents released to media in the past show that the agency

has put a lot of effort into compromising Juniper firewalls and those made by other companies.

An NSA spy tool catalogue leaked to Der Spiegel in 2013 described a sophisticated NSA implant known as FEEDTROUGH that was designed to maintain a persistent backdoor in Juniper firewalls. FEEDTROUGH, Der Spiegel wrote, burrows into Juniper firewalls and makes it possible to smuggle other NSA programs into mainframe computers .. It s also designed to remain on systems even after they re rebooted or the operating system on them is upgraded. According to the NSA documents, FEEDTROUGH had been deployed on many target platforms.

FEEDTROUGH, however, appears to be something different than the unauthorized code Juniper describes in its advisories. FEEDTROUGH is a firmware implant a kind of aftermarket spy tool installed on specific targeted devices in the field or before they re delivered to customers. The unauthorized code Juniper found in its software was embedded in the operating system itself and would have infected every customer who purchased products containing the compromised versions of the software.

Naturally, some in the community have questioned whether these were backdoors that Juniper had voluntarily installed for a specific government and decided to disclose only after it became apparent that the backdoor had been discovered by others. But Juniper was quick to dispel those allegations. Juniper Networks takes allegations of this nature very seriously, the company said in a statement. To be clear, we do not work with governments or anyone else to purposely introduce weaknesses or vulnerabilities into our products Once this code was discovered we worked to produce a fix and notify customers of the issues.

Prins says the larger concern now is whether other firewall manufacturers have been compromised in a similar manner. I hope that other vendors like Cisco and Checkpoint are also now starting a process to review their code to see if they have backdoors inserted, he said.

Oracle Ordered To Publicly Admit Misleading Java Security Updates

Security issues have long tantalized over 850 Million users that have Oracle’s Java software installed on their computers. The worst thing is that the software was not fully updated or secure for years, exposing millions of PCs to attack.

And for this reason, Oracle is now paying the price.

Oracle has been accused by the US government of misleading consumers about the security of its Java software.

Oracle is settling with the Federal Trade Commission (FTC) over charges that it "deceived" its customers by failing to warn them about the security upgrades.

Java is a software that comes pre-installed on many computers and helps them run web applications, including online calculators,

chatrooms, games, and even 3D image viewing.

The FTC has issued a press release that says it has won concessions in a settlement with Oracle over its failure to uninstall older and insecure Java SE software from customer PCs upon the upgrade process, which left up to 850 Million PCs susceptible to hacking attacks.

However, the company was only upgrading the most recent version of the software and ignoring the older versions that were often chock full of security loopholes that could be exploited by hackers in order to hack a targeted PC.

So, under the terms of the settlement with Oracle, announced by the FTC on Monday, Oracle is required to:

- Notify Java customers about the issue via Twitter, Facebook, and its official website
- Provide tools and instructions on how to remove older versions of Java software

Oracle has agreed to the settlement that is now subject to public comment for 30 days, although Oracle declined to comment on its part.

Meanwhile, the FTC wants Java users to know that if they have older versions of the software. Here is the website that will help you remove them: java.com/uninstall.

Apple Blasts U.K. Bill on Backdoor Access to Encrypted Messages

In the wake of a renewed debate over the use of encrypted communications, Apple is urging the British Parliament to reconsider its new beefed-up surveillance proposals.

The company submitted a strongly worded objection to the U.K. s Scrutiny Committee today in a response to a law drafted in November. If passed this spring, the legislation dubbed the Investigatory Powers Bill would legally require companies to bypass encryption at the request of the government, among many other provisions.

The eight-page letter, which was provided to Yahoo News by Apple, argues that the bill in question threatens to hurt law-abiding citizens in its effort to combat the few bad actors who have a variety of ways to carry out their attacks. The California-based company, which has included encrypted privacy measures in its computers and smartphones for over 10 years, argued that forcing backdoors into products would weaken the protections built into Apple products and endanger all our customers.

The move comes amid a heated debate about the use of encryption in consumer technology, spurred by revelations that terrorists may have communicated via encrypted messaging services such as WhatsApp and Telegram prior to the Nov. 13 Paris attacks.

FBI Director James Comey has argued that terrorists are

increasingly using this technology which scrambles the content of a message so that only its sender and receiver can read it to go dark. In a recent Senate hearing, he called on U.S. tech companies that offer end-to-end encryption to rethink their business models, implying they should provide exceptional access to the government when needed. Cryptographers and cybersecurity activists unanimously agree that there s no way to do this without entirely compromising the security of all encrypted communications. Major tech companies, including Google, Microsoft and Facebook, have fought law enforcement in court and at the legislative level over this issue for years.

The United Kingdom is just one of many countries to propose legislation aimed at regulating encryption. Soon after the attacks in Paris, the French newspaper Le Monde published documents discussing potential legislation to forbid free and shared Wi-Fi connections during emergencies and block the use of the Tor anonymity network. (Prime Minister Manuel Valls denies that these proposals ever existed.) In the United States, Sen. Dianne Feinstein, D-Calif., and Senate Intelligence Chairman Richard Burr, R-N.C., recently announced they hope to pass a law that would require companies to decrypt data under court order.

 I think this world is really changing in terms of people wanting the protection and wanting law enforcement, if there is conspiracy going on over the Internet, that that encryption ought to be able to be pierced, Feinstein said earlier this month.

Apple s testimony argued that increasingly stronger not weaker encryption is the best way to protect against terrorist threats. It also recommended that the bill provide more detail on what might be required of those who are served warrants, and parts of it should not apply to overseas providers.

 This would immobilize substantial portions of the tech sector and spark serious international conflicts, it reads. It would also likely be the catalyst for other countries to enact similar laws, paralyzing multinational corporations under the weight of what could be dozens or hundreds of contradictory country-specific laws.

Though Apple does comply with law enforcement requests by providing certain types of metadata, it has also denied court access to encrypted communications that take place in iMessage and FaceTime. This past summer, for instance, the Justice Department obtained a court order for a case involving drugs and guns, demanding Apple turn over real-time text messages between suspects using iPhones. The company responded by saying it could not technically comply.

In another case this fall, Apple said it could feasibly recover information on mobile devices running iOS 7, but because public sensitivity to issues regarding digital privacy and security is at an unprecedented level, doing so could threaten the trust between Apple and its customers and substantially tarnish the Apple brand and ultimately cause a longer term economic impact.

The document emphasizes the technical restrictions Apple faces in carrying out the requests of Parliament, arguing that it is

mathematically impossible to decrypt the data of a few wrongdoers without compromising the company s entire customer base.

The best minds in the world cannot rewrite the laws of mathematics, it reads. Any process that weakens the mathematical models that protect user data will by extension weaken the protection.

The company also said that recent history is littered with cases in which a backdoor was introduced to a company s encrypted product and it was subsequently exploited. One example is Juniper Networks, a tech giant that markets networking products. Last week, the company discovered that an unauthorized backdoor had been embedded in a system running on some of its firewalls, resulting in significantly compromised data.

On Sunday evening, CEO Tim Cook underscored the recommendations of Apple s testimony in a 60 Minutes interview.

If there s a way to get in, then somebody will find the way in, he told Charlie Rose. There have been people that suggest that we should have a backdoor. But the reality is if you put a backdoor in, that backdoor s for everybody, for good guys and bad guys.

He emphasized that denying access to encryption would not necessary mean the nation would be less safe.

I don t believe that the tradeoff here is privacy versus national security, Cook continued. I think that s an overly simplistic view. We re America, we should have both.

Facebook’s Freebie Internet Service Comes Under Fire in India

Facebook’s Free Basics is having some trouble in India, with critics saying the service turns the Net into a walled garden.

Regulators in India want to pull the plug on Facebook’s controversial Free Basics service.

The Telecom Regulatory Authority of India has requested that the sole company in that country to offer Free Basics, which provides rudimentary access to the Internet, put a halt to the program, according to a report in the Times of India.

It’s unclear whether the service is actually accessible at the moment. Wednesday’s report cited an unnamed official who said that the Free Basics provider, Reliance Communications, has complied with the request, but also that its own check showed that the service still seems to be available.

At issue in India is whether the service meets the standards of Net neutrality, the principle that there should be equal access to all types of content and services on the Internet. The Indian regulator reportedly wants Reliance to give it details on the terms and conditions of Free Basics access as the agency weighs

merits of varied pricing for different types of content.

Facebook created Free Basics to provide a set of Internet services in areas including news, maternal health, local jobs and local government information. It has provided those services as part of its Internet.org initiative, which launched in 2014, in countries across Asia, Africa and Latin America where online access has been limited or nonexistent.

But the initiative has been a lightning rod for critics who say it actually gets in the way of a free and open Internet, creating a walled garden favoring Facebook and a small number of online venues. Others have accused Facebook, the world's largest social network, of forcing companies to offer their services at no cost.

In April, several Web publishers in India withdrew from Internet.org, saying Facebook gave preferential treatment to certain sites, services and platforms.

On Wednesday, the Menlo Park, California-based company defended its efforts in India.

"We are committed to Free Basics and to working with Reliance and the relevant authorities to help people in India get connected," a Facebook spokesperson said.

Reliance Communications and the TRAI did not immediately respond to a request for comment.

Google Is Trying To Kill Passwords. But What Should Replace Them?

Google is testing out a new way to sign into their services and it nixes one of the most annoying security measures out there: passwords. The tech giant is trying out a feature that lets some users confirm their identity just by using their smartphones.

The move is not only just the latest sign that the tech industry is trying to get users away from passwords. It's also the latest sign that companies still aren't quite sure how to replace them yet.

Passwords are almost impossible to escape right now, but keeping track of the dozens you need just to navigate your daily online life can be maddening.

And they're also almost universally hated: Creating strong, unique passwords can feel like pulling teeth and reusing them can leave you vulnerable when a service you rely on gets breached. Moreover, data from those almost inevitable breaches shows that people keep sticking to ridiculously easy-to-guess passwords like "123456" or, well, "password."

"Right now it's relatively convenient to have a simple password," said Alvaro Bedoya, the executive director of Georgetown Law's Center on Privacy & Technology. "But as hacks increase and breaches proliferate, people are starting to realize that also

may be dangerous."

Many big sites and services now offer two-factor authentication an added layer of protection that often works by making you enter a code that’s delivered to your phone via text messages or an app.

Google’s new test seems to be a lot like just taking the password part out of this common two-factor equation and it appears to be very similar to a system Yahoo launched for its mail app users earlier this year.

"We’ve invited a small group of users to help test a new way to sign-in to their Google accounts, no password required," a Google spokesperson confirmed, adding that the days of "password" and "123456" are numbered.

The system is pretty straightforward, according to a reddit post from user rp1226 that appears to have first brought the test to light. "You authorize your phone to allow you to log in to your account. You go into a computer and type in your email. Then you get a message on your phone to allow the login. If you hit yes, the computer logs into your Google account without a password," he wrote.

The test works for both Android and iOS devices and users can still use their password to login as normal if they don’t have their phone handy. And you can revoke access to the feature from a device at anytime, according to a copy of documentation accompanying the test posted by the reddit user.

But there are some pitfalls to the phone-only approach: If someone is able to access your phone while it’s unlocked, they could potentially log in to your account. (Although, presumably, if they have your unlocked phone they’ve already gotten to a treasure trove of your personal data that probably includes your inbox.)

Another booming password alternative is biometrics, which use physical characteristics like your fingerprints to prove who you are.

Fingerprint scanning is already happening with newer iPhones around the world and in some workplaces. The method can be appealing because unlike passwords, you aren’t really able to forget your fingerprints. But that’s also a potential problem: Your fingerprints are permanent, so they can’t be changed even if, say, they are among a massive trove of prints compromised by a hack at a major government agency.

And unlike passwords, they aren’t secrets: You leave them on a lot of things you touch and some research has even suggested fakes good enough to fool some systems can be made from high resolution photos of your hands.

Companies are exploring these alternatives because of the obvious issues with passwords and concerns that consumers won’t want to go through the added steps involved in multi-factor verification methods.

But Bedoya says people and companies should think carefully before relying solely on any one type of authentication because they each come with their own risks.

"At the end of the day, the more factors you add the more secure you are," he said.

How to Turn Any Non-Touch Screen PC Into a Touch Screen

Want to buy a touch-screen laptop but couldn’t afford it?

But what if I told you that you can turn your existing non-touch-screen laptop into a Touch Screen laptop?

Yes, it’s possible. You can now convert your laptop or PC into a touch screen with the help of a new device called AirBar.

Touch screen has become a popular feature on laptops these days, and many laptops are moving toward having touch screens, but not every laptop or desktop model comes with the feature.

Swedish company Neonode has brought to you a new device, AirBar, that would bring the touch technology to virtually any computer from your non-touch laptops to notebooks.

What is AirBar and How does it Work?

AirBar is a small plug-and-touch bar that attaches magnetically to the bottom of your machine’s display.

When connected to your laptop via an available USB port, AirBar starts emitting a beam of invisible light across your screen that is used to track touchscreen movements and gestures.

The movements and gestures are then translated into corresponding inputs, making you able to use all the gestures including poking, pinching, swiping, zooming and scrolling around with your hand, in the same way, like on a touchscreen PC.

And What’s Great about AirBar is that

it even works if you have worn gloves, and with any other object.

AirBar works well with any device running Windows 8 or Windows 10 or even with a Chromebook, but it still needs to have proper OS X support.

The AirBar is going to retail for $49 next month with its public launch in January 2016 at the CES event in Las Vegas. 15.6-inch screens size at present. Currently, the only size that AirBar accommodates is 15.6-inch screens.

The First Website Went Online 25 Years Ago Today: Here’s What It Was

Chances are, you’re reading this story on a digital screen.

And whether you’re using a desktop, a tablet or a phone, you might be interested in knowing that the first website went online 25 years ago today, though it looked nothing like the interactive versions you see today.

Tim Berners-Lee’s World Wide Web wasn’t public when it first went live CERN, the European Particle Physics Laboratory in Geneva, Switzerland, on Dec. 20, 1990, Engadget reports, and was little more than an explanation of how the hypertext-based project worked. Even though it didn’t go live until Aug. 6, 1991, that initial version holds the distinction of being the first web page.

The page is a far cry from the modern version, containing little more than linked sentences on a white background.

The initial idea was to allow researchers around the world to share information and it was Berners-Lee who first coined the term "World Wide Web" in 1989. Early version of the website included an explanation of the concept and information for users to create their own sites.

Berners-Lee went on to found the World Wide Web Consortium at the Laboratory of Computer Science at the Massachusetts Institute of Technology in Boston, where he still serves as director.

The actual webpage created by Berners-Lee was put back online at its original address for its 20th anniversary. You can see it here: http://info.cern.ch/hypertext/WWW/TheProject.html

=~=~=~=